IBM Institute for Business Value | Research Insights

Capturing the cybersecurity dividend

How security platforms generate business value

How IBM and Palo Alto Networks can help

IBM Consulting and Palo Alto Networks have joined forces to deliver AI-powered, fully integrated, open, end-to-end security solutions to enterprises. From consultation through execution, we can help you modernize your cybersecurity program, saving time, money, and resources as well as enhancing your organization’s resilience against today’s complex threats. For more information, visit ibm.com/consulting/palo-alto.

Foreword

Organizations around the globe are facing a pivotal moment in security—one that requires urgent action.

Digital connectivity expands attack surfaces and creates new vulnerabilities. Cyberattacks are becoming more sophisticated and harder to defend against. And AI is being used by both defenders and attackers, creating a race in cybersecurity capabilities.

Cybersecurity tools and solutions abound, most promising some sort of sea change. In reality though, many deliver only a ripple or, at best, a passing wave. Why? Complexity is getting in the way of results.

The cybersecurity landscape has always been a complex web of threats and countermeasures. But the proliferation of threats and the mind-boggling number of potential responses today is enough to rob a Chief Information Security Officer or Chief Technology Officer of some much-needed sleep. Organizations juggle an average of 83 different security solutions from 29 vendors. It's unnecessary convolution and risk. More tools equal more threats; every integration is a potential point of entry for bad actors.

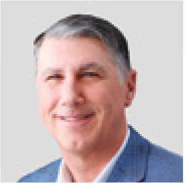
In today's world, effective security requires platformization. Platformized organizations take 72 days less, on average, to detect a security incident and 84 days less to contain one. Consolidating multiple tools into a unified platform not only bolsters security posture, it also reduces costs and improves operational efficiency—two things any C-suite executive or business leader will welcome. And when it comes to AI, a platform approach best enables an organization to ingest and analyze data, and then deliver actionable insights.

Our roles give us an opportunity to engage with organizations from every industry and geography, providing us a view from the security mountaintop—and we see that waiting is a risky game. This isn't just about future-proofing, it's about safeguarding the present. Imagine security tools that harmonize seamlessly, sharing intelligence and automating responses at an unprecedented speed. This vision is already a reality for many organizations that have platformized their security since Palo Alto Networks introduced the concept one year ago.

Security platforms offer unparalleled visibility, strengthened defenses, improved costs, and efficiency—all leading to tangible business benefits. A robust, integrated security platform can be the shield that protects your organization's reputation, customer trust, and bottom line.

In today's AI-fueled world, strong partnerships are more essential than ever. The strategic partnership between IBM and Palo Alto Networks brings together leading security platform, AI, and transformation capabilities. Collaborating on this report, we have identified what it takes to successfully pivot to security platformization and what it can deliver for your organization. Together, we are unique in our ability to help you embrace this opportunity and be the best partners for you.

Mohamad Ali
Senior Vice President and Head
IBM Consulting



BJ Jenkins
President
Palo Alto Networks

Key takeaways

52% of executives say complexity is the biggest impediment to their cybersecurity operations.

- **Security fragmentation is now the unhappy norm.**

  The average organization has 83 different security solutions from 29 vendors. A majority, 52%, of executives say complexity is the biggest impediment to security operations.

- **Security platforms bring faster response times and higher ROI.**

  Platformized organizations take 72 days less, on average, to detect a security incident, and 84 days less to contain one. They also reap an average ROI of 101%, compared to 28% for those that are not yet embracing platformization.

- **Platformization moves the security function from "necessary cost" to value generator.**

  96% of executives in our survey who have adopted platformization say security is a source of value, compared to just 8% of those who haven't.

The average cost of security complexity is more than

5%

of annual revenue.

Cybersecurity should boost the bottom line

As the digital landscape continues to change, organizations face a daunting reality: cybersecurity complexity is eating away at their bottom line.

In fact, cybersecurity is more expensive than ever. The average cost of a data breach rose 10% in 2024, to an all-time high of $4.88 million.[1] And when a growing threat landscape is addressed with more security solutions, an organization's overall security costs rise significantly, with cybersecurity spending expected to grow more than 50% from 2023 to 2025. Meanwhile, 80% of executives agree they face pressure to reduce the cost of security.

The illusion of "more solutions, more security"

Many organizations have continued to add to their stable of security solutions, hoping to plug holes as they become apparent and as threats increase. But our research shows this approach is not a path to success—instead, it adds complexity and inefficiency. There's a limit to how far you can get by adding more security solutions. That strategy gradually dilutes the benefits of each new solution and ultimately reduces security effectiveness (see Figure 1).

So what is the solution? Where is there opportunity, what models exist, and what lessons can they teach? To explore these questions, the IBM Institute for Business Value (IBV) partnered with Palo Alto Networks to survey 1,000 executives involved in security across 21 industries and 18 countries. The results provided some clear opportunities and actionable lessons.

Tellingly, 52% of executives say complexity is the biggest impediment to their cybersecurity operations. When asked to estimate the total impact of security complexity to their business, responses from C-suite executives on the security front line were startling. Based on their responses, the average cost of security complexity is more than 5% of annual revenue. For a company with $20 billion in annual revenue, that's a $1-billion annual cost to the business resulting from security incidents, inefficiencies, failed digital transformation efforts, stalled AI initiatives, loss of customer trust, and reputational damage.

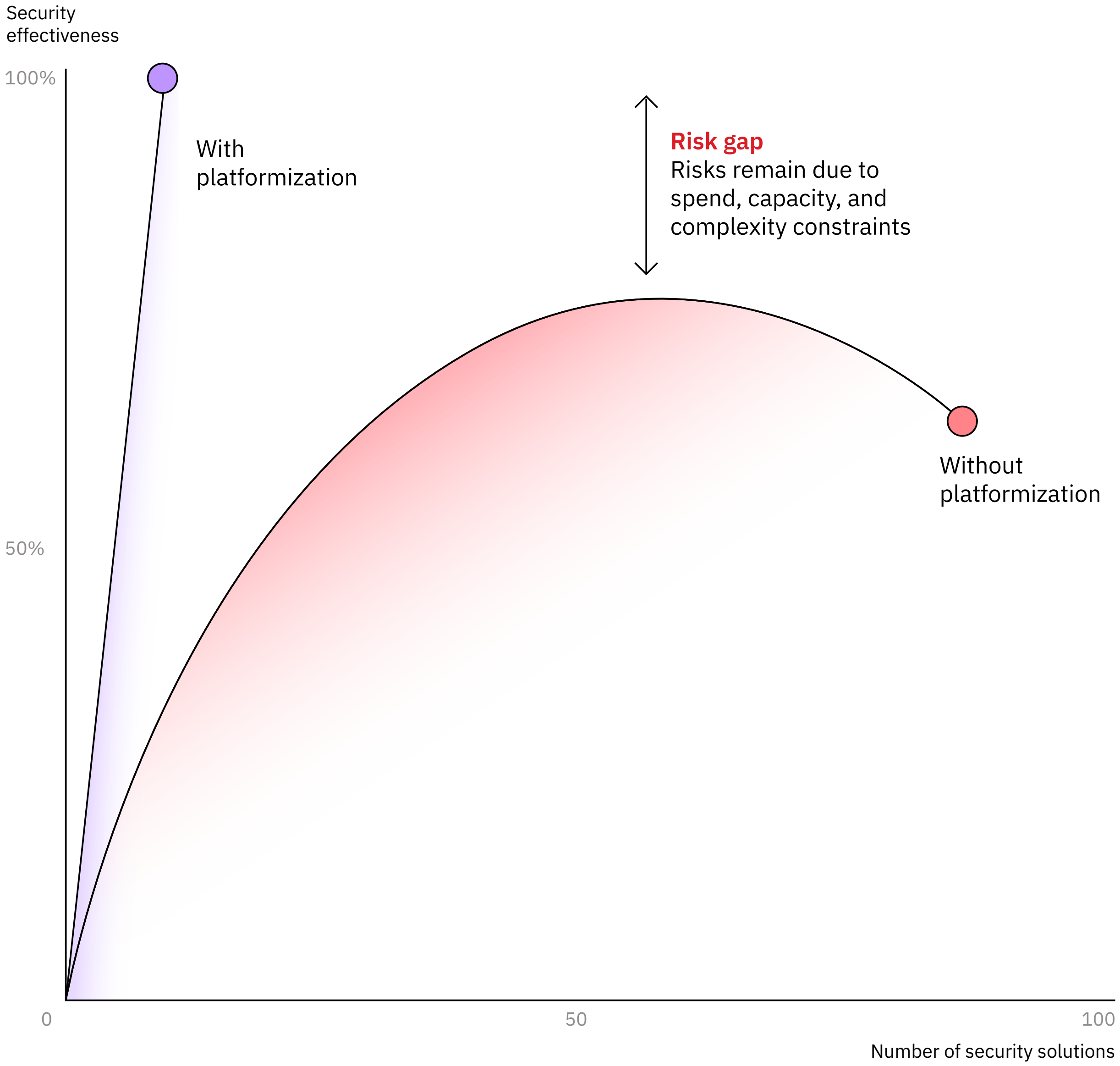
"Cybersecurity is a permanent race."[2]

Hauke Stars

Member of the board, IT & Data
Volkswagen AG

FIGURE 1

Platforms bring fewer point solutions, more effective security overall



The security business challenge facing many leaders:

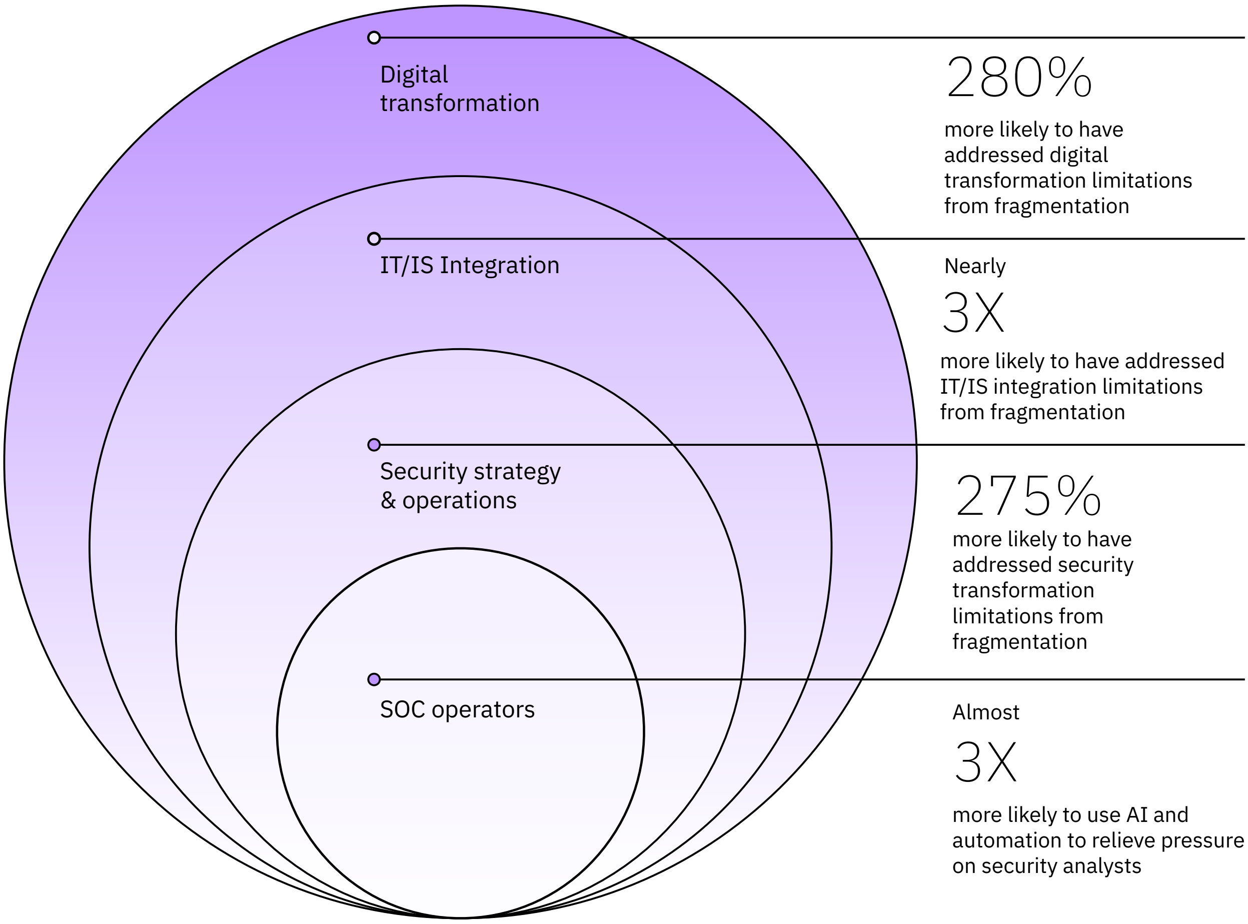
Security complexity directly impacts business factors like ROI.	As the number of security solutions proliferates, more spend is required to achieve fewer outcomes.	This results in a dynamic where complexity feeds itself and leaders can never spend "enough" on cybersecurity.

An antidote to the costs of security complexity

By addressing complexity—strategically consolidating and integrating security solutions onto a common platform—organizations can dramatically lower their risk posture, reduce their costs, and unlock improved business opportunities. We call this security platformization—and our research shows a distinct connection between platformization and positive business and security outcomes (see Figure 2).

FIGURE 2

Platform users gain practical benefits at all levels



280%

more likely to have addressed digital transformation limitations from fragmentation

Nearly

3X

more likely to have addressed IT/IS integration limitations from fragmentation

275%

more likely to have addressed security transformation limitations from fragmentation

Almost

3X

more likely to use AI and automation to relieve pressure on security analysts

70%

less likely to report workload increases from fragmentation

There’s a better way to approach security

This report outlines how a shift in strategic approach to security platformization can generate benefits, plus delves into the significant impacts platformization can have on AI initiatives. In addition, we’ll offer a guide to realize these improvements.

Current security approaches are not a path to success

80% of executives agree they face pressure to reduce the cost of security even as new threats emerge.

74% of executives agree that the current workload on their security operators is excessive.

52% of executives agree that fragmentation of their security solutions is limiting their ability to deal with threats.

Perspective

How we analyzed the impact of security platforms

To assess the role of security platformization in overall security and business performance, we analyzed the 1,000 organizations in our survey set. We developed an index of security platformization based on four key criteria:

- **Simplification.** How great a role does consolidation play in security strategy?
- **Portfolio rationalization.** How consolidated are security tools and technologies?
- **Proactive housekeeping**. How well and regularly are outdated security solutions identified and removed?
- **Platforming progress.** To what extent are security platforms adopted?

For each criterion, executives answered a scaled question assessing their progress. The platformization index was created as a simple average of their scores on each of the four.

Throughout this report, we illustrate the relationship between platformization index scores and performance via scatter diagrams or by segmenting the 1,000 executives into quartiles based on their index scores. The top quartile refers to the organizations with the highest platformization index scores, while the bottom quartile consists of the organizations with the lowest platformization index scores. But it's not where organizations sit on the index that is the nugget of gold in this research—rather, it's the relationship between platformization and various positive outcomes.

Key takeaways from the analysis

Our analysis reveals a strong correlation between the platformization index and key security performance metrics. Organizations with higher platformization scores demonstrate:

- **Faster incident response.** Platformized organizations take 72 days less, on average, to detect a security incident, and 84 days less to contain one.
- **Improved ROI.** An average ROI of 101% compared to 28% for those that are not yet embracing platformization. Platformization explains 48% of the variation in ROI.
- **Enhanced return on security investment (ROSI).** An average ROSI of 116% compared to 32% for those that are not yet embracing platformization. Platformization explains 49% of the variation in ROSI.

In short, the data indicates security platformization helps drive improved performance and optimizes the value of security investments.

Platformized organizations take

72 days less, on average, to detect a security incident, and

84 days less to contain one.

> “When we did all the math, we actually knocked our cost down by several hundred thousand dollars per year. If you looked at all the components that were included, we were able to say it’s not only do we get more, but we pay less.”

Jerry Cochran

Deputy Chief Information Officer; Division Director, Cybersecurity & DigitalOps
Pacific Northwest National Laboratory (US)

> “One of the main benefits of the security platform is that our provider has a roadmap. We can align our strategy to capitalize on that. We gain efficiencies because our security partner is showing us how the solution will evolve. They are making the investments necessary to develop the platform and integrate the different capabilities.”
>
> **Javier Torres Alonso**
>
> Chief Information Security Officer, Allfunds

Digital transformation and platforms: A business performance boost

Rethinking risk

Think about a large construction project with multiple contractors, each using their own tools, materials, and blueprints. While each contractor might be skilled, coordinating their efforts without a unified plan and shared resources can lead to delays, inefficiencies, and potential safety hazards.

The current state of cybersecurity is similar. Organizations have accumulated security products and services over time on a tool-by-tool basis. Each has its own dashboards, data models, training needs, and more. Our research shows that enterprises juggle an average of 83 different security solutions from 29 vendors, creating a tangled, expansive mess that frustrates security professionals and hinders overall effectiveness.

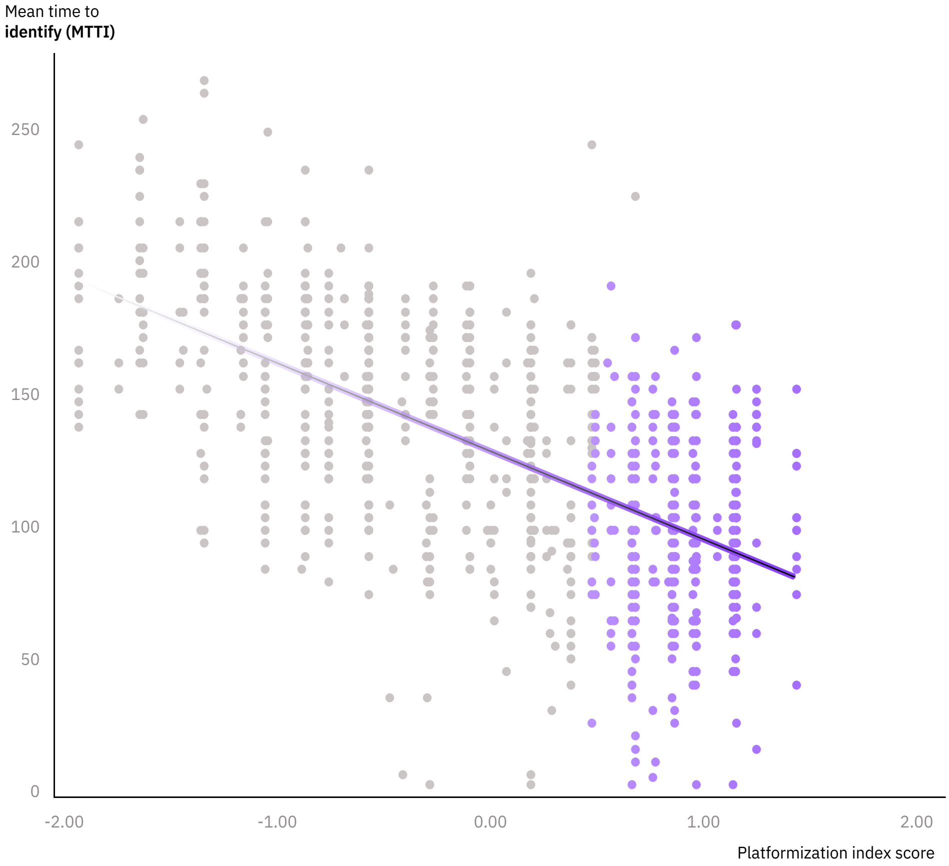
Security platformization is the equivalent of unifying the construction under a single general contractor, with standardized equipment and procedures. Platformization eliminates unnecessary repetition of work, simplifies operations, and empowers security teams to focus on strategic initiatives.

The benefits are compelling. Organizations in our study that have made strides toward platformization report substantially fewer incidents and data breaches. Their mean time to identify (MTTI) or detect security incidents is 72 days shorter, while mean time to contain (MTTC)—the time it takes to resolve an incident—is 84 days less. Also, 80% of platformization adopters in our research say they have full visibility into potential vulnerabilities and threats, versus only 28% of non-adopters.

Our research shows that enterprises juggle an average of 83 different security solutions from 29 vendors.

FIGURE 3

Organizations with the greatest security platform maturity are faster to identify and contain security incidents



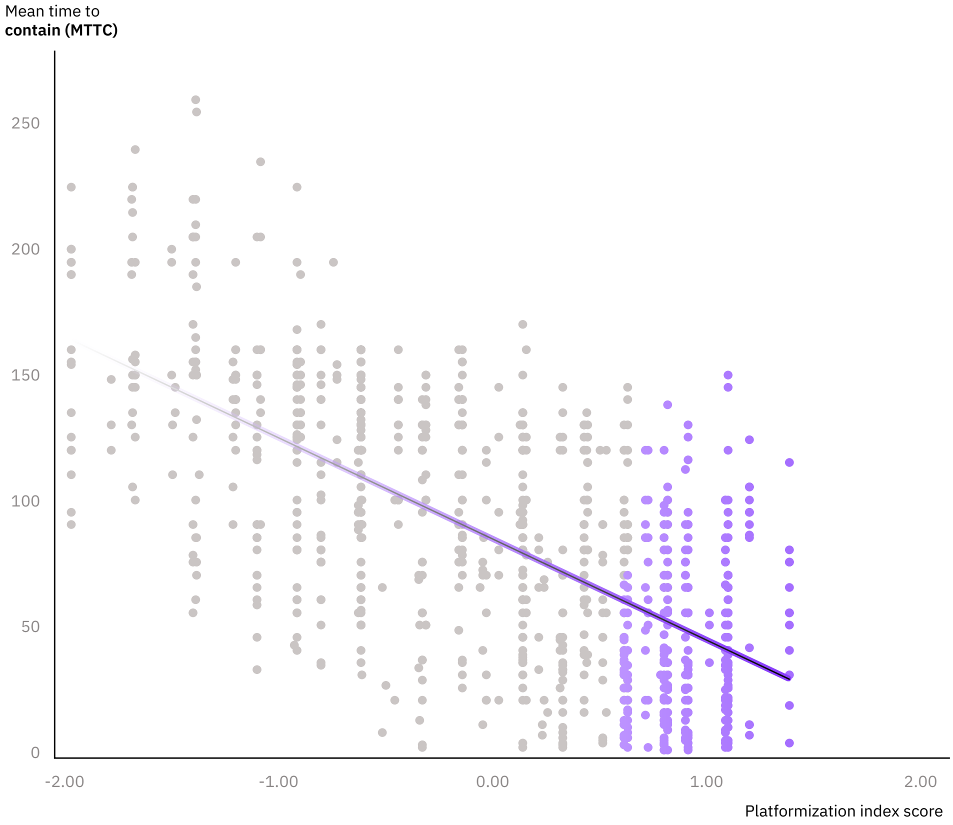
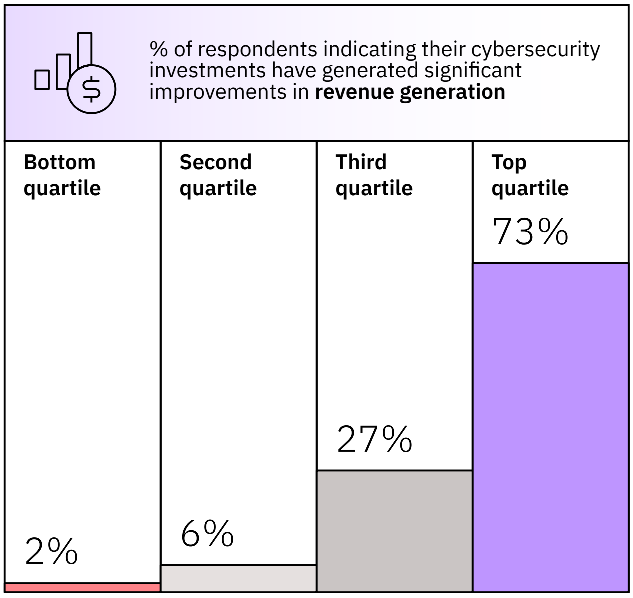
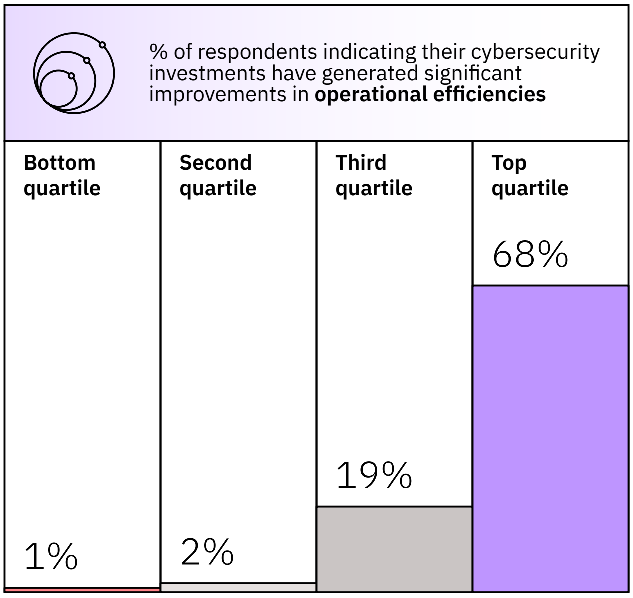


FIGURE 4

Platformized organizations see greater business impact from their cybersecurity investments





Revenue generation and efficiency

Security platformization can further business goals. In fact, in our research, seven out of 10 organizations with a high degree of platformization report that cybersecurity investments have helped revenue generation and operational efficiencies. Only 2% of executives from organizations that have yet to move toward platformization say the same.

This advantage comes in part from enhanced agility. Many digital transformation efforts can be derailed by security concerns. Yet among platform users, only 10% of digital transformation initiatives fail to scale due to security concerns, compared to 26% for non-platform users.

What's more, platformization aids innovation initiatives. Too often, in the normal course of business, cybersecurity is relegated to the role of gatekeeper—a last line of defense that slows down responsiveness and deters experimentation. In contrast, organizations in our study that use integrated security platforms have greater visibility, control, and access to automation. That helps transform security from a cost center to a value driver.

In fact, 96% of executives in our survey who have adopted platformization say security is a source of value, compared to just 8% of those who haven't.

7 out of 10

organizations with a high degree of platformization report that cybersecurity investments have helped revenue generation and operational efficiencies.

Only 2%

of non-platformized organizations report the same.

Action guide

Rationalize your security toolset. Establish a working group with your security, technology, and business leaders to evaluate the impact of security complexity on key performance metrics. Conduct a comprehensive security toolset assessment, including a cost-benefit analysis of each tool. Identify redundancy, gaps, and opportunities for consolidation or replacement.

Pivot to a platform-first approach. Engage the right partner to build a business case for security platformization. Prepare a board-level briefing on operational benefits and cost savings to gain C-suite buy-in. Create a roadmap for scaling your security platform.

Perspective

What defines a good security platform?

Security platforms combine numerous solutions into a tightly integrated architecture that makes the whole (the platform) better than the sum of the parts (the corresponding “best-of-breed” point solutions). The idea of security platformization follows a consolidation logic many organizations have applied to other parts of their business, such as enterprise resource planning (ERP) or customer relationship management (CRM).

Rather than managing security capabilities independently of each other, you can move security capabilities onto a common platform to ensure greater visibility and better governance across the operations lifecycle. Rather than forcing piecemeal parts together to manage your security posture, you let the platform carry the burden. Identity and access management capabilities are informed by zero trust, network segmentation, and endpoint detection and response (EDR) capabilities. The AI-generated insights from your security information and event management (SIEM) solution are available to SOC incident responders. By reducing the number of application integrations, you decrease potential vulnerabilities from misconfigurations and data mismatches. By reducing the number of handoffs, you improve response times and increase accountability.

As you consider platforms, here a few characteristics they should have:

The consolidated platform is as secure or better than the corresponding point products you’re currently using. Adopting a platform should never mean sacrificing security efficacy for simplified management or vendor consolidation.

The platform is modular. It has to be, to allow your organization to grow into the platform over time. You must be able to adopt the platform in whole or in parts, without losing its ability to address the use cases being considered.

It streamlines integrations. Integrations should make each component stronger than it is on its own. All too often, platforms are developed by building a single user interface (UI), but with each product operating entirely independently beneath that UI. While this approach might improve visibility, it fails to capitalize on the more meaningful benefits from architectureal integration and operational standardization. True consolidation involves rethinking technology solutions but also people and support processes. Everything from policy management to reporting must be consolidated and tightly integrated.

"Our security team has to manage multiple environments—hybrid cloud and on premises. And with the platform, for the first time, it feels like we're securing them at the same time and can see real-time what's happening in both. We've enhanced overall security in an integrated way."

Syed Faheem

Information Technology Infrastructure & Operations Manager
muvi Cinemas (KSA)

Building a bridge between information technology and information security

Traditionally, information technology (IT) and information security (IS) have operated in separate silos with different priorities and responsibilities. The move to platformization makes security operations an integral part of the broader IT estate—as much a contributor as a consumer.

Our research shows that 80% of organizations without a unified platform struggle with fragmentation. The lack of cohesiveness for companies that have not adopted platformization can make them vulnerable to potential threats simply because they lack visibility and awareness.

Deliberate, integrated design matters more than ever

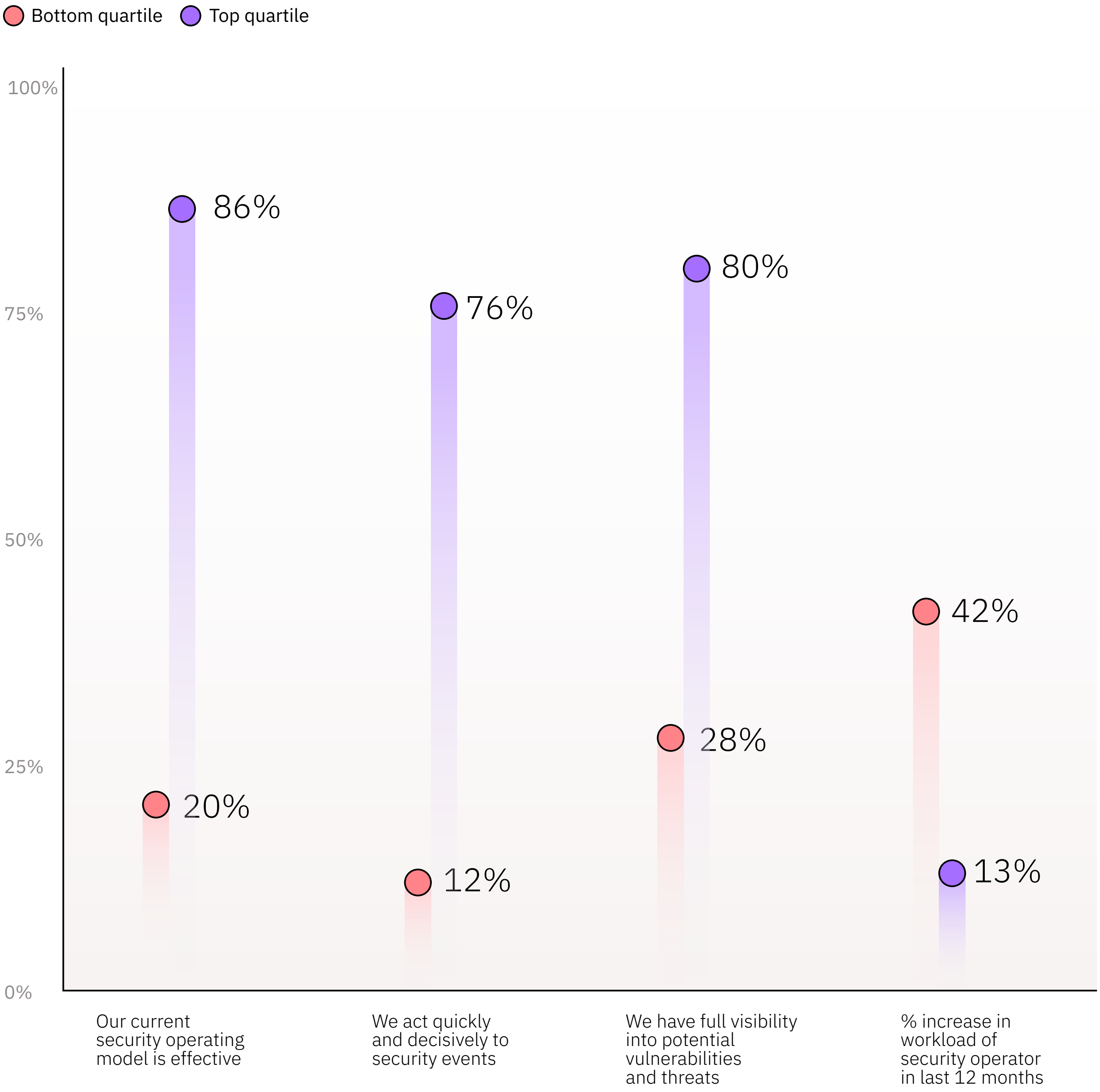
While threat actors are deploying AI and automation capabilities, cyber defenders continue to struggle with skill, capacity, and coordination issues. New tactics like multiple extortion campaigns mean data breaches and ransomware are simply steps in far more sophisticated, coordinated attacks.

Leaders must adopt a new perspective, where IT, IS, and AI capabilities reinforce each other. Within the next two years, 90% of executives expect to be scaling, optimizing, or innovating with AI.[3] A security platform affords the common governance needed to deliver the AI capabilities shaping the future.

As hybrid cloud services become commonplace, and AI operations become the norm, integration runtime capabilities across IT and IS solutions are essential. Three out of four (75%) organizations that have embraced security platformization agree that better integration across security, hybrid cloud, AI, and other technology platforms is crucial. This doesn't just mean integrating the technologies themselves; it involves increased collaboration and rethinking operational governance for a hybrid-cloud-and-AI fueled world. It means spending less time thinking of how to connect solution architecture with operations and more time thinking about improving speed to insight and outcome efficiency.

FIGURE 5

Organizations that move to platforms create more effective, efficient security operations



A security platform affords the common governance needed to deliver the AI capabilities

shaping the future.

> "For us, efficiency and agility are important because our team is not very big. Having a large security solution set means each team member must know more, train more, earn different certifications. Having a single platform makes it much easier for us. It's a way to get everybody on the same page quickly."
>
> **Javier Torres Alonso**
> Chief Information Security Officer, Allfunds

This is where intentional design becomes paramount—and the notion of "hybrid by design" comes into play. Hybrid by design is a strategy for integrating cloud solutions with IT/IS infrastructure, operating models, and ecosystems, ensuring technology aligns with broader business goals.[4] Following a hybrid-by-design approach helps ensure security is baked in from the start, alongside cloud and AI capabilities. By standardizing architecture and operational variables, the security platform becomes a source of greater efficiency and accountability—just as we've seen with ERP and sales platforms.

From risk aversion to value creation

Creating cohesiveness between IT and IS before AI is deployed across your organization can help avoid multiple integration headaches. And new trends are emerging that require IT/IS consolidation for success. For example, zero-trust and network-segmentation use cases require thinking through both IT network architecture and security access controls.

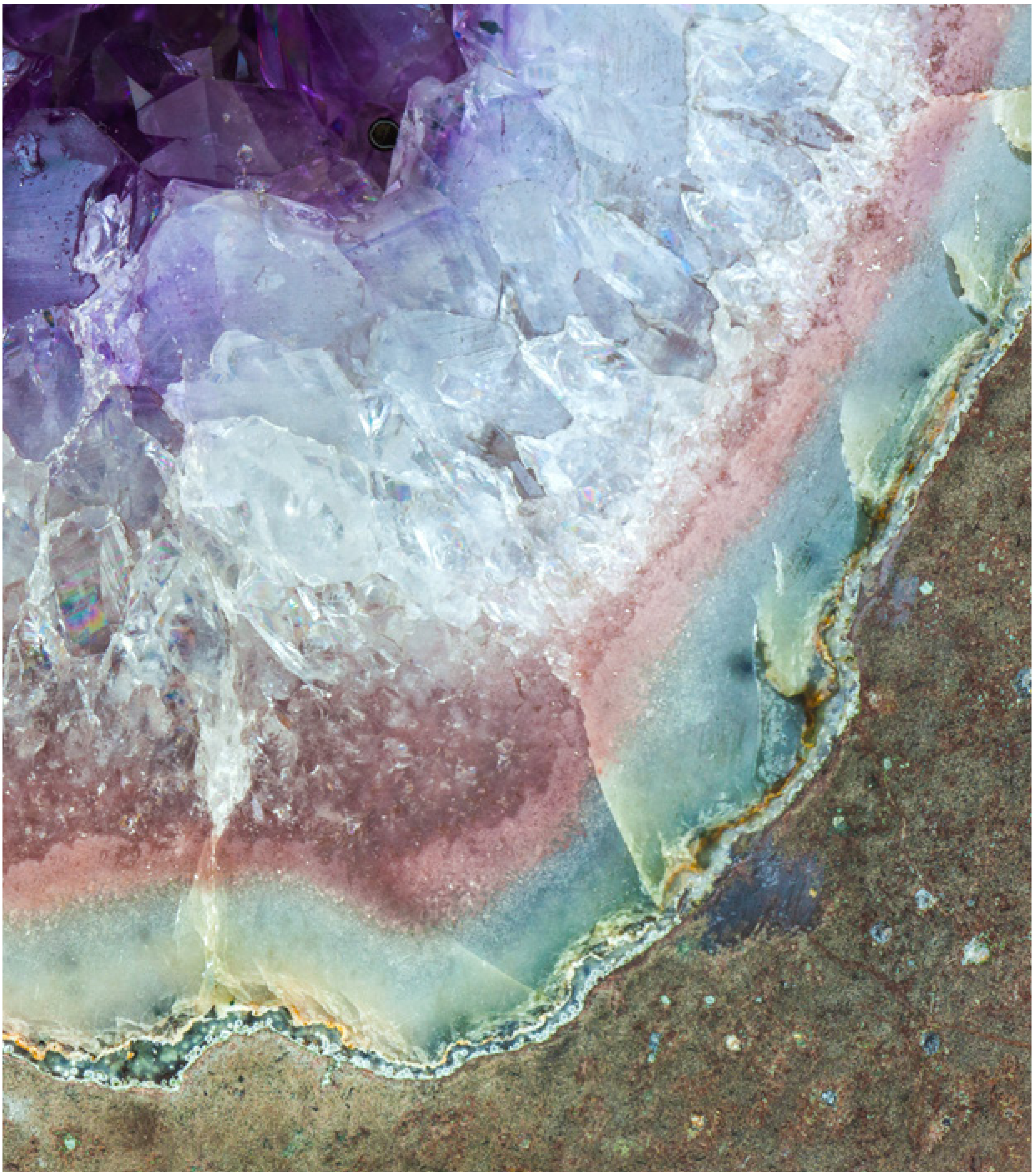
Bridging the gap between IT and IS with a security platform can shift organizational focus from risk aversion to value creation, transforming potential threats into opportunities for innovation and growth. The more teams embrace the use of common platforms and services, the less time they waste getting everyone on the same page. And leaders can spend less time negotiating standards and governance and devote more energy to achieving goals. By removing fragmentation and complexity, a consolidated security platform is key to higher performance.

Action guide

Integrate IT/IS architecture and operations. Create clear standards and common reference patterns for hybrid cloud, AI, and cybersecurity with leaders from IT, IS, and business operations. Design and architect for fast-paced AI threats—using hybrid-cloud capabilities to accelerate integration and orchestration across the security lifecycle.

Extend your capabilities through partners. Visit a cyber range to assess how AI threats are evolving; use it to support continuous improvement, training, and change management as you transform your security operating model with platformization. Engage a preferred managed security services partner (MSSP) to accelerate your AI transformation.

While 4 out of 5 non-platform users agree their security operators cannot deal effectively with the sheer quantity of threats and attacks, only one in five platform users think the same.



> “I think everybody desires not to have 29 panes of glass. It’s inefficient from a staffing, training, and hiring perspective because I’ve got to have an ABC expert and an XYZ expert and so on. So I can buy these tools piecemeal from multiple vendors or I can buy one platform, get unsurpassed integration, and increase my efficiency.”

Jerry Cochran

Deputy Chief Information Officer; Division Director, Cybersecurity & DigitalOps
Pacific Northwest National Laboratory (US)

Streamlined security strategy and operations

The security operations center (SOC) is the beating heart of cybersecurity, but only 51% of organizations believe their current security operating model is effective. By reinforcing better ways of working, platforms can drive efficiency and visibility. In fact, 98% of organizations with a mature approach to platformization agree their security processes are efficient and clear, compared to just 32% of those without platformization.

Platformization also slashes security procurement costs by eliminating overlapping functionality, providing greater accountability on spend and reducing overall maintenance costs. Of non-adopters, 41% say security fragmentation has driven up procurement costs.

Organizations that tap platformization actually spend less on cybersecurity as a percentage of their IT budget than others. But they achieve much greater impact with their spend, seeing an average ROI four times better than non-adopters.

Platforms can aid efficiency by easing workload demands on security operators and freeing up human capital for transformation efforts and other digital advances. While four out of five non-platform users agree their security operators cannot deal effectively with the sheer quantity of threats and attacks, only one in five platform users think the same.

98%

of organizations with a mature approach to platformization agree their security processes are efficient and clear, compared to just 32% of those without platformization.

Perspective

The performance boost of platformization in different industries

Industries differ greatly in terms of investment, capabilities, and performance, but when it comes to longer dwell times, everyone's at risk. Dwell time, the amount of time a cyber attacker stays undetected within a network or system, means more risk exposure. And when it comes to performance, greater operational complexity makes a big difference. More solutions mean more complex infrastructure and integrations, which can lead to more vulnerabilities and more challenging governance.

In the banking and financial markets sector, leading security platformization adopters are the top performers when it comes to threat management metrics. They're seeing a 57% improvement in performance compared to non-adopters in their industry for mean time to identify and contain a breach.

On the other hand, the manufacturing sector is dealing with the longest time to identify and contain breaches. But even here, security platformization is making a difference. Leading platformization adopters in this sector are seeing a 32% performance boost compared to those that have yet to adopt platformization.

Regardless of industry, platformization is giving organizations a notable performance improvement.

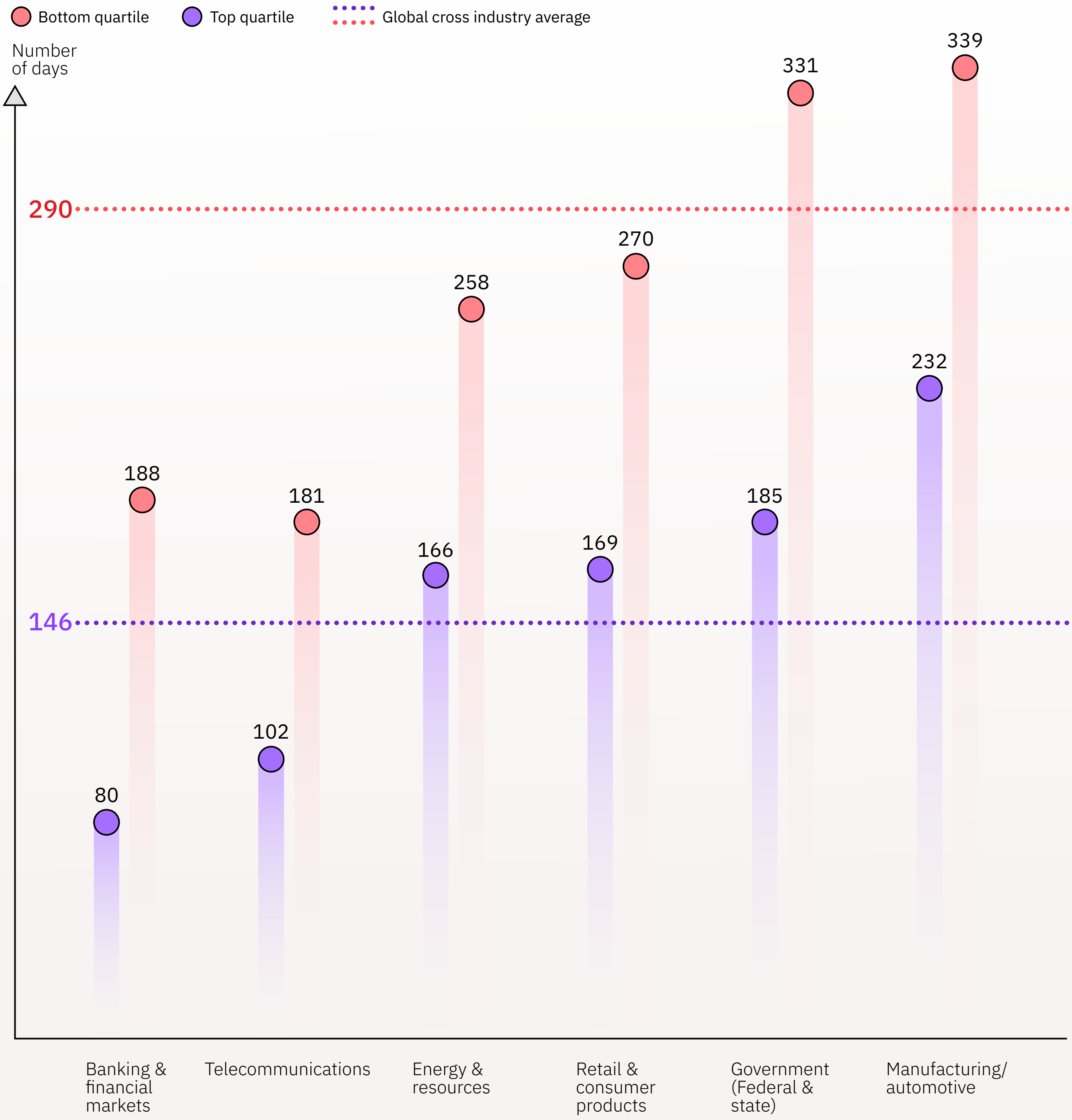
> "The platform simplifies the work of our security analysts. Our incident response team now has time to take action more proactively. They have the time to look into things more deeply. They can focus more on the complex security issues."

Syed Faheem
Information Technology Infrastructure & Operations Manager
muvi Cinemas (KSA)

FIGURE 6

Security platformization performance by industry

Mean Time To Identify (MTTI) plus
Mean Time To Contain (MTTC)



Case study

Better gets better with integrated security platform

Founded in 2016, Better has funded more than $100 billion in home loans, furthering its mission to transform the mortgage industry and make owning a home simpler and faster. However, along with rapid growth and the launch of new services, Better also experienced an increased tempo of cyberthreats, which increased the manual burden on security employees.

And with thousands of remote employees logging in every day, the firm also had to protect a rapidly expanding potential attack surface. In the financial services industry, highly sensitive data and management of customer and employee accounts must be kept secure. Data security is key to building customer trust and managing compliance with state and federal regulations.

To adopt a more mature approach to threat detection and response—and automate processes to make its SOC team more effective and efficient—Better deployed an integrated platform of solutions for network, cloud, endpoints, and security operations. Each security solution was configured to reduce friction and increase collaboration between business and engineering teams.

Today, instead of managing security solutions piecemeal from several different security vendors, Better now benefits from a unified security platform—a scalable platform that can provide secure access from virtually anywhere, facilitate visibility and control over cloud security, and deliver substantially lower costs than its previous multivendor approach.

By decreasing incident-response time, automating 90% of responses, and reducing investigation times from hours to minutes, Better's IT team now has significantly more time to focus on security strategy and manage more complex, emergent threats.

> By decreasing incident-response time, automating
>
> 90%
>
> of responses, and reducing investigation times from hours to minutes, Better's IT team now has significantly more time to focus on security strategy and manage more complex, emergent threats.

Spending more?

Spending less?

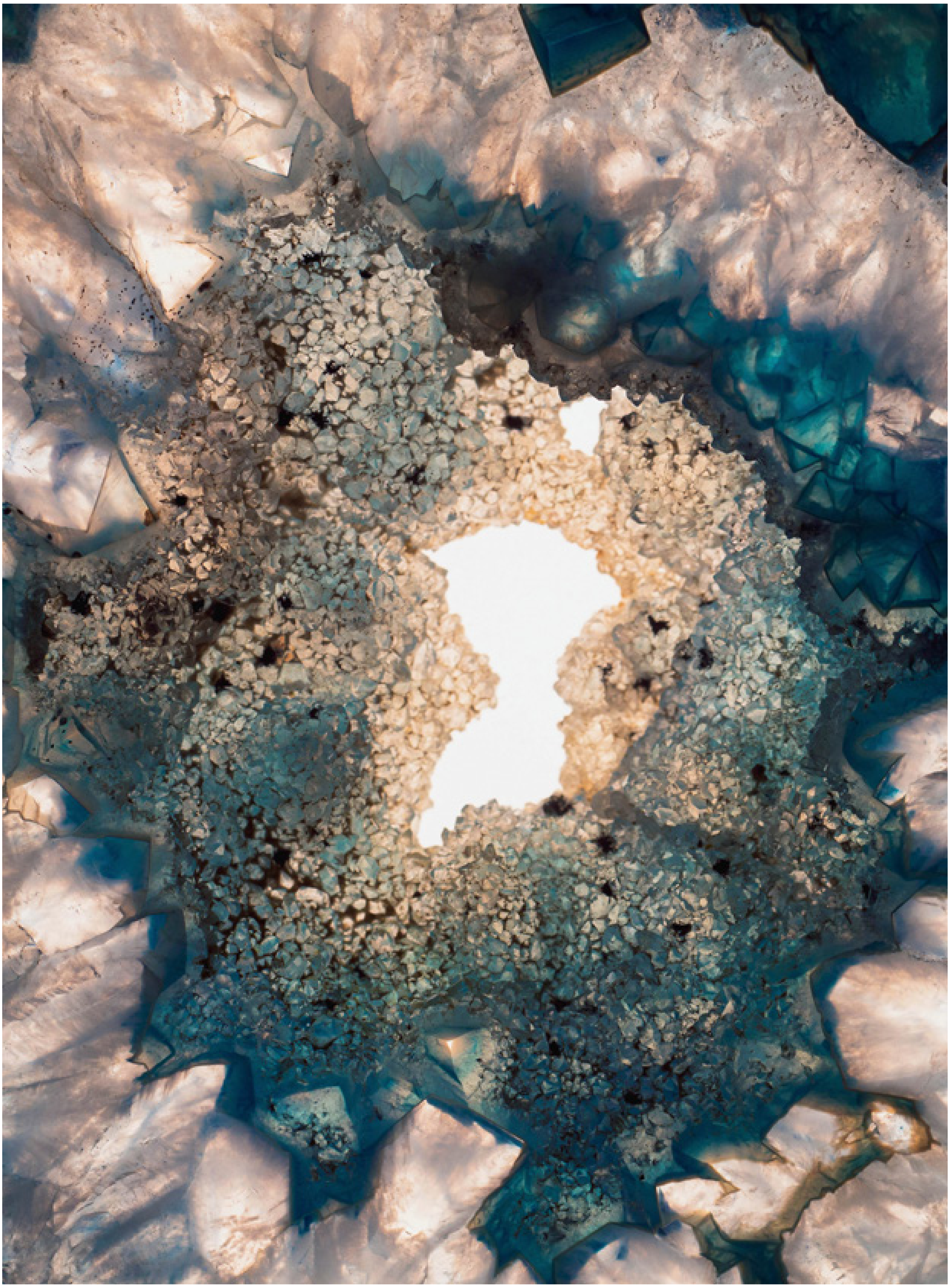
Or just spending better?

Organizations that tap platformization actually spend marginally less on cybersecurity as a percentage of their IT budget than others. And they spend better, achieving greater impact. These organizations have an average ROI on security investment of 101% compared to 28% for those that are not yet embracing platformization.

Action guide

Choose partners that streamline your security mission and trim those that don’t. Critically evaluate current and potential partners in terms of technology, services, and support and make hard decisions about where to double down and where to break up.

Run your playbook. Stage incident-response drills to assess where a unified platform can deliver greatest impact. Identify sources of friction and where decisions are impaired by lack of data or poor workflow management. Take remedial actions to improve your incident-response capabilities.



Roughly

8 out of 10

executives in our research agree that adopting security platforms will improve AI operations across the enterprise.

AI-fueled security platforms are supercharging security teams

Today's cyberthreats are too complex and too fast-moving for reactive security. To stay ahead, organizations need a proactive, intelligent, AI-fueled defense.

Imagine AI as a tireless guard integrated into your security platform, constantly scanning your network for vulnerabilities. It sees patterns humans can't, predicts attacks before they happen, and suggests countermeasures. AI can provide a holistic and dynamic view of the entire security posture, with insights and recommendations derived from endpoints, networks, servers, cloud workloads, and security information and event management systems (SIEMs).

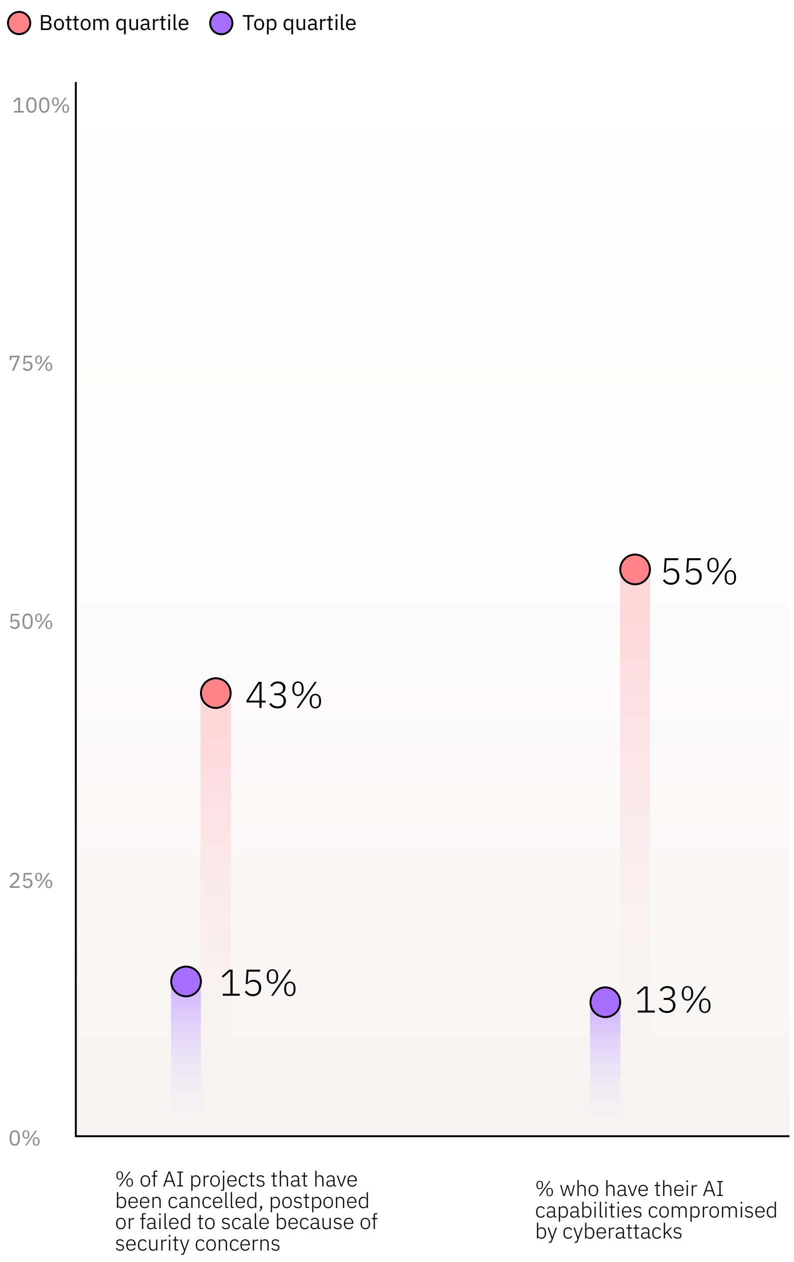
Our research shows security platformization users are better able to tap this potential. To make AI truly effective as a security tool, it's crucial to ingest data from multiple data sources—proprietary, second- and third-party, regulated, etc. Securing both the infrastructure and the data-in-motion requires comprehensive visibility—something a unified platform can provide.

Platformization can reduce the pressure on individual operators by creating a more integrated toolbox—starring AI—that improves visibility across threat vectors, geographies, and technology platforms. It unifies data to help uncover the source of emerging threats and provides operators with near-instantaneous visibility and responsiveness. Our analysis reveals that organizations using platformization are far less likely to report fragmentation and lack of transparency among their security teams. In contrast, 82% of organizations with low platform adoption indicate their security analysts' performance is hindered by a lack of visibility and transparency.

A security platform can also help protect and advance additional AI business initiatives throughout the organization. Roughly eight out of 10 executives in our research agree that adopting security platforms will improve AI operations across the enterprise. A platform approach allows organizations to embed security into their AI initiatives from the outset, helping ensure that security is not an afterthought. And organizations that tap security platformization see substantially fewer of their AI initiatives compromised by security-related issues (see Figure 7).

FIGURE 7

Organizations that have adopted security platformization are better able to execute their AI agenda



Action guide

Elevate your security operators with AI and automation. Use a security platform to democratize AI capabilities for all your security operators, mitigating capacity and skill constraints. Extend your reach with ecosystem partners by using platform services to accelerate adoption of agentic AI.

Modernize your security posture to support AI everywhere. Establish common governance and support processes to accelerate response times. Determine what combination of automation and augmentation delivers the best operational and security outcomes.

Integrated security platforms: A gateway to opportunity

By embracing security platformization, you can elevate security from a cost center to a strategic asset.

Using a platform to reduce the security complexity so many organizations currently struggle with brings benefits beyond the individual organization. Platformization also makes it easier to integrate security capabilities into ecosystem partnerships. Almost all organizations that use security platforms (99%) agree they can easily integrate new entities and business units into their security organization, compared to only 40% of those who have not embraced security platformization.

To do so effectively, the security platform must be an integral part of your organization's overall IT architecture. When built on an open hybrid-cloud architecture and powered by AI, security platformization becomes a catalyst for your business and security transformation. It can link your hybrid cloud, AI, and security capabilities and help make your enterprise secure by design. It links your hybrid cloud, AI, and security capabilities, makes your enterprise secure by design, and accelerates your journey to next-generation security.

> When built on an open hybrid-cloud architecture and powered by AI, security platformization becomes a catalyst for your business and security transformation. It can link your hybrid cloud, AI, and security capabilities and help make your enterprise secure by design.

Authors

Mark Hughes

Global Managing Partner
Cybersecurity Services
IBM
linkedin.com/in/markhughesibm/

Karim Temsamani

President
Next Generation Security
Palo Alto Networks
linkedin.com/in/karim-temsamani/

Contributors

Sara Aboulhosn
Associate Creative Director, IBM Institute for Business Value

Sheryl Chamberlain
Managing Director, Global Alliances (IBM), Palo Alto Networks

Liam Cleaver
Research Director, IBM Institute for Business Value

Rob Daniels
Director GSI Business Development, Palo Alto Networks

Jacob Dencik
Research Director, IBM Institute for Business Value

Angela Finley
Design Lead, IBM Institute for Business Value

Hebatallah Nashaat
Data and Content Management Manager, IBM IBV

Gerry Parham
Global Research Leader, IBM Institute for Business Value

Lily Patel
Senior Analyst, IBM Institute for Business Value

Calvin Person
Director Solutions Architect, Palo Alto Networks

Rob Rachwald
Director of Product Marketing, Palo Alto Networks

Kristine Rodriguez
Editor-in-Chief, IBM Institute for Business Value

Research methodology

New data and findings in this paper are from a recent survey conducted by IBM Institute for Business Value in collaboration with Oxford Economics. From July through September 2024, 1,000 executives across 21 industries and 18 countries were surveyed. In addition to descriptive analysis, we analyzed data from the executives to facilitate the creation of a "platformization index." This index measures the extent to which an organization has moved toward security platformization. Based on the index, regression analysis was conducted to ascertain the relationship between security platformization, and security and business outcomes. In addition, moderator and mediator analysis was conducted to understand how platformization interacts with other capabilities in supporting security outcomes. To facilitate the presentation of our data analysis, we segmented results from the platformization index into quartiles showing the extent of security platformization progress. These quartiles were used to further understand differences in performance as well as practices and approaches for enabling next generation cybersecurity.

About Research Insights

Research Insights are fact-based strategic insights for business executives on critical public- and private-sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions. From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights. To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also find us on LinkedIn at https://ibm.co/ibv-linkedin.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

Related reports

Unify your fragmented security: Accelerate transformation with platformization
IBM Institute for Business Value. May 2024.
https://ibm.co/next-gen-platform-cybersecurity

6 blind spots tech leaders must reveal: How to drive growth in the generative AI era (Tech CxO study)
IBM Institute for Business Value. August 2024.
https://ibm.co/c-suite-study-ceo

The CEO's guide to generative AI: Cybersecurity
IBM Institute for Business Value. October 2023.
https://ibm.co/ceo-generative-ai-cybersecurity

Architecting for AI agility: How hybrid by design can help tech architectures accelerate business outcomes
IBM Institute for Business Value. July 2024.
https://ibm.co/hybrid-by-design-agile-tech-architecture

Notes and sources

[1] Cost of a Data Breach Report 2024, IBM and Ponemon Institute. 2024. https://www.ibm.com/reports/data-breach

[2] Ali, Mohamad, Varun Bijlani, John Granger, Matt Hicks, Ric Lewis, Salima Lin, Aparna Sharma, Joanne Wright, and Kareem Yusuf. *The Great Tech Reset: How hybrid by design creates business value.* IBM Institute for Business Value. IBM Corporation. November 2024

[3] Five Trends for 2025 study. IBM Institute for Business Value. n=400. November 2024. Unpublished data.

[4] Ali, Mohamad, Varun Bijlani, John Granger, Matt Hicks, Ric Lewis, Salima Lin, Aparna Sharma, Joanne Wright, and Kareem Yusuf. *The Great Tech Reset: How hybrid by design creates business value.* IBM Institute for Business Value. IBM Corporation. November 2024.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | January 2025

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.